Dartmouth College HANOVER • NEW HAMPSHIRE • 03755-3529
Office of the Provost • 6004 Parkhurst Hall, Rm. 204 • Tel (603)646-4091 • Fax (603)646-3773
martin.n.wybourne@Dartmouth.edu

Martin N. Wybourne
Vice Provost for Research
Francis and Mildred Sears Professor of Physics

Senator Tom Coburn, MD
Chairman
Subcommittee on Federal Financial Management
439 Hart Senate Office Building
Washington, D.C., 20510

Attn: Anna Shopen,
Fax: (202) 228-3796

1 September 2006

Dear Senator Coburn,

I am writing on behalf of Dartmouth College in response to your letter of July 27, 2006, requesting information on research supported by appropriations. Given the academic calendar and timing of the request, it is difficult for me to provide all of the detail requested, but I will try to address the key concerns of your letter.

Dartmouth College does not use a federal lobbyist and has no plans to engage one. As Vice Provost for Research, I am responsible for federal government relations and believe it is important for faculty members and administrators to work directly with congressional delegations on issues that affect higher education. My work with the New Hampshire congressional delegation is guided and informed by an internal committee of the most senior academics and administrators at Dartmouth.

Dartmouth has received appropriation funding during the past six years, particularly in support of cyber security and first responder programs in two institutes: The Institute for Security Technology Studies (ISTS), established in 2000 as a principal national center for counter terrorism technology and cyber security research, and the Institute for Information Infrastructure Protection (I3P), established in early 2002 as a consortium that brings experts together to identify and help mitigate threats aimed at the U.S. information infrastructure. The I3P was formed following a President's Committee of Advisors on Science and Technology recommendation (1998), an Institute for Defense Analyses study (2000), and a National Security Council Office of Science and Technology Policy white paper calling for its creation (2000). Details of ISTS and the I3P may be found at: http://www.ists.dartmouth.edu/ and http://www.thei3p.org/ respectively.

The ISTS comprises mainly Dartmouth faculty, research scientists and students, while the I3P is a national consortium managed by the College. The I3P currently has 29 members representing 15 states. The members are non-profit organizations, government laboratories and leading universities as shown on the attached membership list. Over the past six years funding has been approximately $59 million for the ISTS and $27 million for the I3P. It is important to note that while Dartmouth manages all of the I3P activities and is engaged in I3P research projects, the majority of the funds for the I3P are re-distributed to the other 28 consortium members. Both institutes have established independent review procedures to make recommendations on technical issues and funding levels, and our federal program managers have final approval over all projects.

Researchers in the two institutes have produced many important innovations that include new digital forensics tools, new tools for training first responders, new technology to protect process control systems for the oil and gas industry, and new tools to estimate the cyber security risks associated with business investment decisions. As part of these programs we have worked with Fortune 500 chief information security officers, as well as other senior executives and engineers from multi-national oil and gas companies and software security companies, local and national first-responder organizations, and local and federal law-enforcement agencies. Innovations resulting from the work have benefited many areas. A few specific examples include:

- Digital image forensics work that has led to new software tools to detect photographic image tampering or detect the presence of hidden messages in digital media. These tools have wide application in law enforcement, homeland security and scientific research. Federal agencies and major corporations have provided additional funding to turn research prototypes into production software tools. The FBI's forensics audio, video and image analysis unit has also requested these tools. Ongoing ISTS funding supports the extension of this work to audio and video forensics, and to identifying the digital camera used to take a given photograph.

- A program to provide terrorism-response training and support infrastructure for first responders - the Virtual Terrorism Response Academy (VTRA). The New York State Office of Homeland Security responded enthusiastically to a briefing about VTRA. Officials there have asked to participate in VTRA's beta test period, and have requested that our faculty provide "train the trainer" sessions and an extensive VTRA pilot program.

- ISTS provided the software tools and analysis for a cyber exercise *Livewire* that involved over 50 organizations and 300 people nationwide representing government agencies, the White House (NSC, OMB, HSC, OSTP), two major cities and their state governments, finance and multi-state information sharing and analysis centers, a number of telecommunications firms, hardware and software manufacturers, ISPs, a large energy supplier, a national bank, a securities exchange and others. The scenario involved a nation-state launching a coordinated cyber attack against key infrastructure to put pressure on the U.S. economy and to disrupt recovery at the federal, state and local levels. An after-action report detailing the findings was submitted to the Department of Homeland Security in March 2004.

- I3P researchers are working closely with senior executives at an oil refinery in Mississippi to tie high-level business priorities with specific components of process control system risks.

- As part of a larger I3P effort, researchers at MIT Lincoln Laboratory are working with a major process control system vendor to integrate a new source-code checking tool into the vendor's next product cycle.

- As part of a larger I3P effort, the University of Tulsa is working with a major software security vendor to develop a suite of tools for securing communication networks used in industrial control systems. This work includes the development of a passive scanner to monitor Modbus and DNP3 (protocols used only in process control system environments) traffic for malicious activity, and an active scanner to map the network status.

- I3P is working with industry bodies and technology companies to make a business case for the use of the Domain Name System Security Extensions (DNSSEC) that will strengthen the security of the Domain Name System (DNS) used on Internet-Protocol (IP) networks. DNSSEC is important for securing the Internet as a whole, but faces technical and policy challenges that I3P is working to address.

The ISTS and I3P work has been reported in numerous peer-reviewed articles, conference proceedings, technical reports, and the news media, and a number of books are in preparation for leading scientific publishers. Many undergraduate and graduate students, and post-doctoral fellows, have been educated through ISTS and I3P activities. This cohort is helping to build the next generation of professionals who have the cross-disciplinary knowledge and skills required to work in the burgeoning cyber security field.

Dartmouth is proud of the societal value and impact of the ISTS and I3P research programs. The College upholds the highest academic and ethical standards for all of its research and educational activities and we are constantly striving to improve their quality and maintain their relevance through rigorous internal and external review processes. We will continue our process of reviewing ISTS and the I3P to ensure they maintain the highest standards and develop new knowledge that will benefit the nation.

I hope this information is helpful. Please do not hesitate to let me know if you have any questions.

Sincerely yours,

Martin Wybourne

Cc: President James Wright
Provost Barry Scherr

The I3P Consortium Membership

1. Purdue University (West Lafayette, Indiana)
   Center for Education and Research in Information Assurance and Security (CERIAS)
2. University of Idaho (Moscow, Idaho)
   Center for Secure and Dependable Systems, Microelectronics Research and Communications Institute
3. University of Tulsa (Tulsa, Oklahoma)
   Center for Information Security
4. University of California at Davis (California)
   Computer Security Research Laboratory
5. Cornell University (Ithaca, New York)
   Computing and Information Science
6. George Mason University School of Law (Arlington, Virginia)
   Critical Infrastructure Protection Project (CIPP)
7. Georgia Institute of Technology (Atlanta, Georgia)
   Information Security Center
8. Carnegie Mellon University (Pittsburgh, Pennsylvania)
   H. John Heinz III School of Public Policy and Management
9. Johns Hopkins University (Baltimore, Maryland)
   Information Security Institute - Affiliate Member
10. Oregon State University (Corvallis, Oregon)
    Information Security Laboratory - Affiliate Member
11. University of Illinois (Urbana-Champaign, Illinois)
    Information Trust Institute
12. New York University (New York, NY)
    Institute for Civil Infrastructure Systems
13. Dartmouth College (Hanover, New Hampshire)
    Institute for Security Technology Studies (ISTS)
14. Lawrence Berkeley National Laboratory (Berkeley, California)
15. Los Alamos National Laboratory (Los Alamos, New Mexico) - Affiliate Member
16. MIT Lincoln Laboratory (Cambridge, Massachusetts)
17. MITRE Corporation (Bedford, Massachusetts and McLean, Virginia)
18. Mitretek Systems (Falls Church, Virginia) - Affiliate Member
19. Pacific Northwest National Laboratory (Richland, Washington)
20. RAND Corporation (Santa Monica, California)
21. Sandia National Laboratory (Albuquerque, New Mexico)
22. Columbia University (New York, NY)
    School of Engineering and Applied Science
23. Carnegie Mellon University (Pittsburgh, Pennsylvania)
    Software Engineering Institute - Affiliate Member

24. Indiana University (Bloomington, Indiana)
    School of Informatics
25. SRI International (Menlo Park, California)
26. Stanford (California)
    Computer Science Department - Affiliate Member
27. United States Military Academy (West Point, New York)
28. University of California at Berkeley (California)
29. University of Virginia (Charlottesville, Virginia)